

Device-independent randomness extraction for arbitrarily weak min-entropy source

Jan Bouda,^{1,2,3} Marcin Pawłowski,^{4,5} Matej Pivoluska,¹ and Martin Plesch^{1,6}

¹*Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic*

²*Física Teórica: Informació i Fenòmens Quàntics Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain*

³*LIQUID: Lepanto Institute for Quantum Information and Decoherence, Carrer de Lepant 307, 08025 Barcelona, Spain*

⁴*Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*

⁵*School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*

⁶*Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia*

Expansion and amplification of weak randomness plays a crucial role in many security protocols. Using quantum devices, such procedure is possible even without trusting the devices used, by utilizing correlations between outcomes of parts of the devices. We show here how to extract random bits with an arbitrarily low bias from a single arbitrarily weak min-entropy source in a device independent setting. To do this we use Mermin devices that exhibit super-classical correlations. Number of devices used scales polynomially in the length of the random sequence n . Our protocol is robust, it can tolerate devices that malfunction with a probability dropping polynomially in n at the cost of a minor increase of the number of devices used.

High quality randomness is a very useful resource in many computation and cryptographic tasks. In fact it has been shown that many protocols (including quantum ones) vitally require perfect randomness for their security[1–3].

Unfortunately, at the same time perfect randomness is very rare. In the classical world the true randomness, i.e. independent uniformly distributed random bits, cannot be produced at all. The only available resource is pseudo-randomness, sequences that appear random to all observers (often referred to as adversaries) not having full information about the whole environment. Thus classical randomness generators produce pseudorandom numbers stemming from external sources and fluctuations, hoping that the adversary will not be able to reconstruct all the background information. Sources producing imperfect randomness even taking into account the limited capabilities of the adversary are called weak random sources. To enhance the quality and security of these sources, randomness extractors are used. These are devices that combine more sources of randomness to obtain fewer bits of higher quality [4].

On the other hand, theoretically the production of true randomness is possible, if one assumes Quantum theory to be valid: Preparation of a pure state and measurement in its complementary basis will yield a perfectly random result. This is due to the inherent randomness present in Quantum theory itself - this principle is being used in the design commercially available devices [5]. The assumption, however, is high quality and stability of quantum devices in an adversarial setting, which is far from trivial to achieve [6].

In addition, quantum devices in reality act more like black boxes that are inaccessible for users except for providing them classical inputs and obtaining classical outputs from them. It is very hard, if not impossible, to directly test what these devices actually do, whether they perform operations and measurements as promised and

whether their outputs really come from quantum measurements. Therefore it is crucial to test these devices even during their activity - satisfying these tests shall guarantee that the devices are correctly designed and manufactured and they work as desired. This is possible by utilizing super-classical correlations of certain quantum states - if the device consists from separate parts, their classical results can be tested for correlations and their level, if breaking the classical bound, can be a guarantee of their quantum nature. Using non-trusted (or self-testing) quantum devices is referred as Device independence in a broader scope. The process of transformation of a weak random source into uniformly random bits is called *randomness extraction* throughout this letter.

Weak random sources – To provide a figure of merit of randomness extractors, one needs to characterize the randomness of the input random source. One of the possible parameterizations is the so called Santha–Vazirani (SV) parametrization [7], given by the following property: Let $X = (X_1, X_2, \dots)$ be an arbitrarily long random bit string produced by an ε -SV source. Then for any $1 \leq i \leq n$ it holds that

$$\begin{aligned} \forall x_1, \dots, x_{i-1} \in \{0, 1\}, \forall e \in \mathcal{I}(E), \\ \left| P(X_i = 0 | X_{i-1} = x_{i-1}, \dots, X_1 = x_1, E = e) - \frac{1}{2} \right| \leq \varepsilon, \end{aligned} \quad (1)$$

where E is any information an adversary Eve might hold. Note here that the apparent randomness (i.e. without knowledge of E) of each X_i may as well be uniform. The purpose of introducing random variable E is to represent possible correlations between the choice of the measurement settings and internal workings of the devices running a Bell type test.

Second possibility is to consider a one-shot use source that would produce n -bit strings X (with n being arbitrary large). Here we can characterize the randomness of the source by the (conditional) min-entropy of the pro-

duced sequence defined as

$$H_\infty(X|E) = -\log_2 \max_{x \in \mathcal{I}(X), e \in \mathcal{I}(E)} P(X = x|E = e).$$

A source is called an (n, k) source if $H_\infty(X|E) \geq k$ and might be also characterized by its min-entropy rate $R = k/n$.

Combining these two approaches we get the reusable min-entropy source with n -bit blocks of output with guaranteed min-entropy k . Such a source can be modeled as a sequence of n -bit random variables X_1, X_2, \dots , such that

$$\begin{aligned} \forall x_1, \dots, x_{i-1} \in \{0, 1\}^n, \forall e \in \mathcal{I}(E), \\ H_\infty(X_i | X_{i-1} = x_{i-1}, \dots, X_1 = x_1, E = e) \geq k. \end{aligned} \quad (2)$$

Therefore, each new block has a guaranteed minimal min-entropy, even conditioned on the previous ones and any information of the adversary. It is easy to see that SV sources are recovered with $n = 1$ and $\varepsilon = 2^{-H_\infty(X)} - \frac{1}{2}$. Source of this type is also called *block source*.

Classically the task of transforming a single weak source, characterized either as a Santha-Vazirani source, or a min-entropy (block) source into a fully random bit is known to be impossible [4, 7]. However, with non-classical resources the task becomes possible. More precisely, weak random source can be used to choose measurements for a Bell test in order to certify that observed correlations cannot be explained by local theories and thus must necessarily contain intrinsic randomness.

In their seminal paper Colbeck and Renner [8] showed that amplification of Santha-Vazirani sources is possible for a certain range of parameter ε and thus opened a line of research devoted to SV amplification. Subsequent works provided protocols that are able to amplify SV-sources for any $\varepsilon < \frac{1}{2}$ in various settings [9–12]. This line of research culminated in the work of Brandão et. al. [13], who showed how to amplify such source of randomness with the use of only eight non-communicating devices. Their work was quickly followed by that of Coudron and Yuan [14], who showed how to use 20 non-communicating devices to obtain arbitrary many bits from a Santha-Vazirani source.

On the other hand, extraction from min-entropy sources is relatively unexplored. There is a sequence of works exploring the validity of Bell tests if the measurements are chosen according to a min-entropy source [15, 16] and the authors of this paper provided a protocol which uses 3-party GHZ-paradox to amplify sources with min-entropy rate $R > \frac{1}{4} \log_2(10)$ against quantum adversaries [17]. Recently an extensive work on this topic was made public on pre-print archive [18]. In this letter we conclude this work by providing a protocol extracting random bits from min-entropy sources of randomness with any non-zero min-entropy rate.

Device-independent concept and Mermin inequality – In this letter we use the three partite Mermin inequality.

ity. Let's consider three spatially-separated boxes, each of them having a single bit input and a single bit output. Let us denote the input bits of the respective boxes by X, Y and Z and the corresponding output bits A, B and C . By construction we guarantee $X \oplus Y \oplus Z = 1$, i.e. we consider only inputs $XYZ \in \{111, 100, 010, 001\}$ simultaneously passed to all boxes. The value v of the Mermin term is a function of the 4 conditional probabilities defined by the behaviour of the device and of the probability distribution p on inputs

$$\begin{aligned} v = & P(A \oplus B \oplus C = 1 | XYZ = 111)P(XYZ = 111) + \\ & + P(A \oplus B \oplus C = 0 | XYZ = 100)P(XYZ = 100) + \\ & + P(A \oplus B \oplus C = 0 | XYZ = 010)P(XYZ = 010) + \\ & + P(A \oplus B \oplus C = 0 | XYZ = 001)P(XYZ = 001). \end{aligned} \quad (3)$$

In particular, for the uniform input distribution we set $P(XYZ = 111) = P(XYZ = 010) = P(XYZ = 001) = P(XYZ = 100) = \frac{1}{4}$ and denote the Mermin term by v_u .

Assuming the uniform distribution on all four inputs, the maximal value of v_u achievable by a classical device [19] is $\frac{3}{4}$ (thus the Mermin inequality reads $v_u \leq \frac{3}{4}$) and there exists a classical device that can make any 3 conditional probabilities simultaneously equal to 1. In the quantum world we can achieve $v_u = 1$ and satisfy perfectly all 4 conditional probabilities using the tripartite GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and measuring σ_X (σ_Y) when receiving 0 (1) on input.

The beautiful property of the Mermin inequality is that the violation v gives us directly the probability that the device passes a specific test $A \oplus B \oplus C = X \cdot Y \cdot Z$. The probability of failing the test reads $w = 1 - v$.

Mironowicz, Gallego and Pawłowski (MGP) [10] showed the following result: Take a linearly ordered sequence of k Mermin devices $D_1 \dots D_k$ (k being arbitrary) that have uniform distribution on inputs, and each device knows inputs and outputs of its predecessors (for optional cheating purposes), but devices cannot signal to its predecessors. Let us assume that the inputs of devices are described by random variables XYZ_1, \dots, XYZ_k , and the outputs by ABC_1, \dots, ABC_k . Then there exists a function $f(\varepsilon)$ such that if the value of the Mermin variable (3) using uniform inputs is at least $v_u \geq f(\varepsilon)$, then the output bit A_k has a bias at most ε conditioned on the input and output of all its predecessors and the adversarial knowledge. This function can be lower bounded by a Semi-Definite Program (SDP) using any level of the hierarchy introduced in [20]. By using the second level of the hierarchy one can obtain the bound on $f(\varepsilon)$ as a function of ε shown in Fig.1. We can set $k = 1$ (having just a single device) and get the lower bound on the detection probability of producing a bit biased by more than ε , which is $w_u > 1 - f(\varepsilon)$. More independent non-communicating devices can be ordered into any sequence

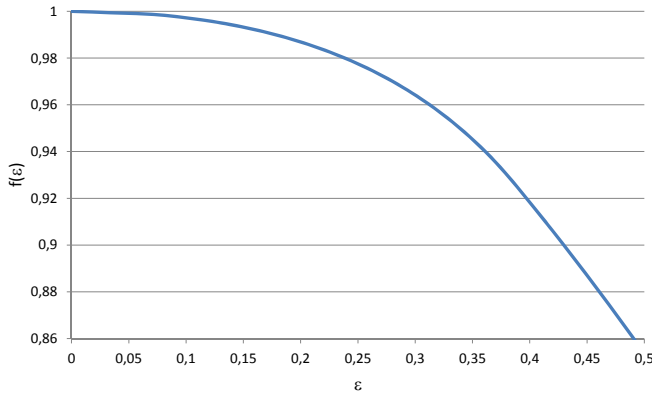


FIG. 1. Depicted is the value of Mermin variable $v = f(\varepsilon)$ needed to certify the bias of the output bit to be at most ε .

and thus this limit holds for any of these devices simultaneously.

Single-round protocol – In the rest of our analysis we will be working with (n, k) sources for an arbitrary n and $k \geq 2$. This is to simplify the explanation, since by taking $\lceil \frac{2}{k'} \rceil$ blocks of an arbitrary (n', k') source with $k' > 0$ we get a (n, k) source with $n = \lceil \frac{2}{k'} \rceil n'$ and $k = \lceil \frac{2}{k'} \rceil k' \geq 2$.

Let us start with a min-entropy $(n, 2)$ source (recall that (n, k) source with $k > 2$ is also an $(n, 2)$ source) and define $N = 2^n$. Let $H = \{h_1, \dots, h_m\}$ be a family of hash functions s.t. $h_i : \{0, \dots, N-1\} \rightarrow \{0, 1, 2, 3\}$. Each hash-function h_i is used to provide input for a Mermin-type device D_i , where outputs of the function 0, 1, 2, 3 identify 111, 100, 010, 001 inputs for the device.

We want to construct H with the property that for every 4-element set $S \subseteq \{0, \dots, N-1\}$ there exist at least one hash function $h \in H$ such that $h(S) = \{0, 1, 2, 3\}$. This is trivially satisfied for the set of all possible hashing functions $H_{full} = \{0, 1, 2, 3\}^N$, however, such a class of functions with its 4^N elements is unpractically large. In the supplementary material we show a construction with logarithmic number of functions in N , thus the number of devices needed scales polynomially with the length of the sequence n . We also stress that for large n one hash function covers as many as 9% of all four-tuples, independently on n . So the size of an optimal set of hash functions might not depend on n at all.

The protocol works as follows:

1. We obtain the (weakly) random n bit string X from the random number generator.
2. Into each device D_i we input the 3 bit string $h_i(X)$ – inputs X_i , Y_i and Z_i and obtain the outputs A_i , B_i and C_i .
3. We verify whether for each device D_i the condition $Z_i \oplus Y_i \oplus X_i = A_i \cdot B_i \cdot C_i$ holds. If this is not true, we abort the protocol due to cheating attempt of the provider.

4. We define the output bit of the protocol as $b = \bigoplus_{i=1}^m A_i$.

The protocol is depicted in the Fig. 2.

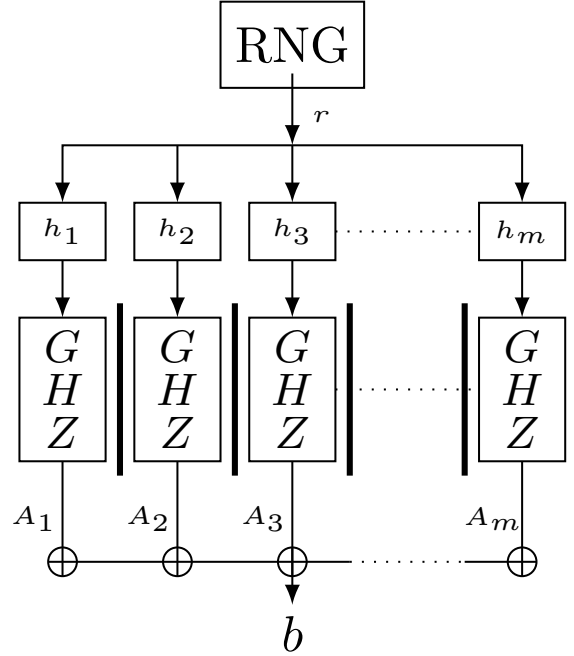


FIG. 2. Depiction of a single round protocol. Bit string drawn from the flat random source is hashed into m inputs into Mermin devices so that at least one device receives perfectly random distribution. This guarantees at least one result almost perfectly random, what also holds for the product of individual results.

Let us now examine the properties of the bit b . First consider only flat $(n, 2)$ distributions. Recall that these are exactly distributions that are uniform on 4-element subsets of the sample space. Our construction of the class H of hash functions assures that for any flat probability distribution there is a function $h_j \in H$ and the corresponding device D_j such that inputs of D_j (hashed by h_j) are uniform on this flat distribution. This gives us that if adversary restricts himself to flat distributions and wants to achieve bias greater than ε for the output bit b , she must achieve this bias in all rounds. The probability that she is not detected while doing this is $v_u \leq f(\varepsilon)$ for each round. The same condition holds then also for the product of all output bits b .

The set of all $(n, 2)$ distributions is convex and flat distributions are exactly all extremal points of this convex set. Thus any $(n, 2)$ distribution d can be expressed as a convex combination of at most N $(n, 2)$ flat distributions d_i (Caratheodory theorem) as $d = \sum_{i=1}^N p_i d_i$ for some $p_i \geq 0$, $\sum_{i=1}^N p_i = 1$. The probability that the adversary is not detected is given by the successful cheating proba-

bilities when using flat distribution $d_i \in \{d_i\}_{i=1}^N$ averaged though the probability distribution on these flat distributions $v_u \leq \sum_{i=1}^N p_i P(\text{not detected} | d_i) \leq f(\varepsilon) \sum_{i=1}^N p_i$ [21]. Thus the upper bound $v_u \leq f(\varepsilon)$ holds for non-flat distributions as well.

To summarize this part, having an (n, k) source with $k \geq 2$, with a single round of a protocol, we can produce a single bit that is biased at most by ε with a certainty of $1 - f(\varepsilon)$.

Multiple-round protocol for block sources – Let us state the most general task: we have an (n, k) block source with arbitrary n and $k \geq 2$ (recall that any source with $k > 0$ can be multiplied to obtain $k \geq 2$). We would like to produce a bit that is biased by no more than ε with certainty of at least $1 - \delta$.

If the one-round version does not meet these parameters, we will repeat the whole protocol l times. By using new devices and new outputs of the block source, each of the runs j will produce a bit b_j , that is biased by ε from perfectly random bit conditioned on all the previous bits up to a probability $f(\varepsilon)$. Thus also the XOR of all output bits $b = \bigoplus_{j=1}^l b_j$ will have at most the bias ε .

After l rounds, the probability of the adversary not being detected will be upper bounded by $f(\varepsilon)^l$. Note that the product form does not come from the fact that the detection probabilities are independent (they are not). This is a product of a chain of conditional probabilities. Recall that the bound $f(\varepsilon)$ holds conditioned by any inputs and outputs of the previous devices (in an arbitrarily ordering that respects the causality). Thus choosing $l > \frac{\log \delta}{\log f(\varepsilon)}$ will guarantee the fulfillment of the conditions for the parameters ε and δ .

Summing up, with an (n, k) block source and $O\left(\frac{\log \delta}{\log f(\varepsilon)} \text{Poly}\left[n \left\lceil \frac{2}{k} \right\rceil\right]\right)$ Mermin devices we can produce a single random bit with bias smaller than ε with probability larger than $1 - \delta$. For producing more bits we simply repeat the whole procedure: all the bits produced will have bias smaller than ε conditioned on the bits produced so far, with linearly scaling of resources.

Protocol for one-shot min-entropy sources – We can model a different scenario where the random source is described by a single use min-entropy source characterized by its min-entropy rate R . In such a case we cannot use the same scenario as before, as there are no independent blocks of randomness with guaranteed min-entropy available. In spite of this fact randomness extraction is still possible on the cost of increasing the number of devices used.

We can draw a bit string from the source with length n and min-entropy Rn , securing at least 2^{Rn} realizations of the string appearing with non-zero probability. We shall use this string for a single round of the protocol, however using a full set of hashing functions H_{full} . Then, for flat sources, there will be at least $\frac{Rn}{2}$ devices obtaining

perfectly random distribution on inputs independently on each other (see supplementary material for explicit construction), yielding failure probability of the protocol $\delta < f(\varepsilon)^{\frac{Rn}{2}}$. Thus choosing $n > \frac{2}{R} \frac{\log(\delta)}{\log(f(\varepsilon))}$ will produce a random bit biased by no more than ε up to a probability δ , though on the costs of double-exponential number of devices in $\frac{1}{R}$ and $\frac{\log(\delta)}{\log f(\varepsilon)}$. For non-flat sources the same result holds due to Caratheodory theorem mentioned earlier.

Robustness – Aborting the protocol after even a single mistake of the devices is certainly highly impractical from the implementation point of view. Therefore we expand our analysis into a situation where we tolerate certain noise on the devices, which would manifest itself by occasional failing of the test condition even for honest devices. More specifically, we shall tolerate a certain fraction of the devices to malfunction without aborting the protocol.

In the supplementary material we show that we can tolerate up to $l \frac{(1-f(\varepsilon))}{2}$ devices to fail in the whole protocol and still achieve the same result as for the perfect protocol by choosing $l > \frac{8 \ln \delta}{f(\varepsilon)-1}$. This translates into increasing the number of rounds of the protocol comparing to the case of ideal devices by a factor of $\frac{8 \ln(f(\varepsilon))}{f(\varepsilon)-1}$. For small ε the parameter $f(\varepsilon)$ approaches 1 and the multiplication factor saturates by 8. For honest devices with individual failure probability bounded by $\frac{(1-f(\varepsilon))}{4m}$, the probability of a false alarm decreases exponentially with the number of protocol rounds l .

Conclusion – In this letter we have introduced a protocol that extracts weak randomness obtained from a min-entropy source in the device independent setting. The protocol works for arbitrarily weak both single-use and block min-entropy sources, with a reasonable scaling of the number of devices in the latter case. Our protocol is also robust, as it allows tolerating some fraction of malfunctioning devices at the cost of a constant increase of the number of devices used.

Acknowledgements – Authors thank P. Horodecki, A. Winter, and S. Massar for insightful and stimulating discussions and Piotr Mironowicz for supplying the raw data for Fig.1. JB, MP2 and MP3 acknowledge the support of the Czech Science Foundation GA CR project P202/12/1142 and support of the EU FP7 under grant agreement no 323970 (RAQUEL). MP3 acknowledges VEGA 2/0072/12. JB acknowledges support by the European Research Council through Advanced Grant "IRQUAT". MP1 acknowledges FNP TEAM, NCN grant 2013/08/M/ST2/00626 and ERC QOLAPS.

-
- [1] J. L. McInnes and B. Pinkas, in *Crypto'90* (1991) pp. 421–435, INCS 537.
 - [2] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, *Phys. Rev. A* **86**, 062308 (2012).

- [3] M. Huber and M. Pawłowski, Phys. Rev. A **88**, 032309 (2013).
- [4] R. Shaltiel, in *Automata, Languages and Programming*, Lecture Notes in Computer Science, Vol. 6756, edited by L. Aceto, M. Henzinger, and J. Sgall (Springer Berlin Heidelberg, 2011) pp. 21–41.
- [5] “Id quantique;” Quantis.
- [6] R. Solcà, *Testing of a quantum random number generator*, Master’s thesis, ETH Zürich (2010).
- [7] M. Santha and U. V. Vazirani, Journal of Computer and System Sciences **33**, 75 (1986).
- [8] R. Colbeck and R. Renner, Nature Physics **8**, 450 (2012), arXiv:1105.3195 [quant-ph].
- [9] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín, Nature Communications **4**, 2654 (2013), 10.1038/ncomms3654, arXiv:1210.6514 [quant-ph].
- [10] P. Mironowicz and M. Pawłowski, “Amplification of arbitrarily weak randomness,” (2013), arXiv:1301.7722 [quant-ph].
- [11] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan, “Free randomness amplification using bipartite chain correlations,” (2013), arXiv:1303.5591 [quant-ph].
- [12] R. Ramanathan, F. G. S. L. Brandao, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki, “Robust Device Independent Randomness Amplification,” (2013), arXiv:1308.4635 [quant-ph].
- [13] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki, “Robust Device-Independent Randomness Amplification with Few Devices,” (2013), arXiv:1310.4544 [quant-ph].
- [14] M. Coudron and H. Yuen, “Infinite Randomness Expansion and Amplification with a Constant Number of Devices,” (2013), arXiv:1310.6755 [quant-ph].
- [15] D. E. Koh, M. J. W. Hall, Setiawan, J. E. Pope, C. Marletto, A. Kay, V. Scarani, and A. Ekert, Phys. Rev. Lett. **109**, 160404 (2012).
- [16] L. P. Thinh, L. Sheridan, and V. Scarani, Phys. Rev. A **87**, 062121 (2013).
- [17] M. Plesch and M. Pivoluska, “Single Min-Entropy Random Sources can be Amplified,” (2013), arXiv:1305.0990 [quant-ph].
- [18] K.-M. Chung, Y. Shi, and X. Wu, “Physical Randomness Extractors,” (2014), arXiv:1402.4797 [quant-ph].
- [19] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [20] M. Navascués, S. Pironio, and A. Acín, New Journal of Physics **10**, 073013 (2008), arXiv:0803.4290 [quant-ph].
- [21] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, Phys. Rev. A **74**, 042339 (2006).
- [22] J. Naor and M. Naor, SIAM J. Comput. **22**, 838 (1993).

Construction of the class H

Let $H = \{h_1, \dots, h_m\}$ be a family of hash functions s.t. $h_i : \{0, \dots, N-1\} \rightarrow \{0, 1, 2, 3\}$. Let us assume that we receive an element of $\{0, \dots, N-1\}$ drawn randomly according some (non-uniform) distribution with min-entropy $\log_2 k$ (we consider only $k \geq 4$).

We want to construct H with the property that for every set $S \subseteq \{0, \dots, N-1\}$ with $|S| \geq k$ there is at least

one hash function $h \in H$ such that $h(S) = \{0, 1, 2, 3\}$. This is trivially satisfied for $H_{full} = \{0, 1, 2, 3\}^N$, however, such a class of functions is unpractically large, it has 4^N elements. Therefore we shall construct a smaller set fulfilling the condition.

Derandomization construction of the class H

Let us consider a sequence of random variables $Z = (Z_0, \dots, Z_{N-1})$ such that $Z_i \in \{0, 1, 2, 3\}$. The outcomes of such a random experiment are N -position sequences from the set $\{0, 1, 2, 3\}^N$. It is easy to see that each such sequence specifies uniquely a particular function $h : \{0, \dots, N-1\} \rightarrow \{0, 1, 2, 3\}$, and vice versa. Since now on we will use them interchangeably.

Let us assume that random variables Z satisfy the condition that for every 4-tuple of positions j_0, j_1, j_2, j_3 and every 4-element string $a_0 a_1 a_2 a_3 \in \{0, 1, 2, 3\}^4$ it holds that

$$P[Z_{j_0} = a_0 \wedge Z_{j_1} = a_1 \wedge Z_{j_2} = a_2 \wedge Z_{j_3} = a_3] > 0. \quad (4)$$

Note that for our purposes even a weaker assumption on Z is sufficient: It is enough if for every 4-tuple of positions j_0, j_1, j_2, j_3 there exists at least one 4-element string $a_0 a_1 a_2 a_3 \in \{0, 1, 2, 3\}^4$ with all a_0, a_1, a_2, a_3 begin mutually different and satisfying (4). However, the stronger condition will make it easier to find a suitable set.

Let us denote $H = \{a \in \{0, 1, 2, 3\}^N \text{ s.t. } P[Z = a] > 0\}$. Using the probabilistic method we see, that for each 4-tuple of positions j_0, j_1, j_2, j_3 and every 4-element string $a_0 a_1 a_2 a_3 \in \{0, 1, 2, 3\}^4$ there exists a function $h \in H$ such that

$$h(j_0) = a_0 \wedge h(j_1) = a_1 \wedge h(j_2) = a_2 \wedge h(j_3) = a_3.$$

The number of functions in H is the same as the number of (nonzero probability) sample space elements of Z . It remains to construct Z with a sample space as small as possible.

Construction of a random variable Z

Definition .1 We define the distance of two distributions D_1 and D_2 by

$$\|D_1 - D_2\| = \sum_{\omega \in \Omega} |D_1(\omega) - D_2(\omega)|,$$

where Ω is the set of all possible events.

Definition .2 Binary random variables are *k-wise δ -dependent* iff for all subsets $S \subseteq \{0, \dots, N-1\}$, $|S| \leq k$

$$\|U(S) - D(S)\| \leq \delta,$$

where $U(S)$ is a uniform distribution over $|S|$ -bit strings and $D(S)$ is a marginal distribution over subset of variables specified by S .

Theorem .3 *The logarithm of the cardinality of the sample space needed for constructing N k -wise δ -dependent random variables is $O(k + \log \log N + \log \frac{1}{\delta})$ [22].*

Let us consider two sequences X_0, \dots, X_{N-1} and Y_0, \dots, Y_{N-1} of binary 4-wise δ -dependent random variables, both sequences being mutually independent. Let $Z_i = 2X_i + Y_i$.

As both X and Y are δ -dependent, their distance from the uniform distribution on every subset of size at most 4 is at most δ . Assuming there is a zero probability for at least one binary string out of $\{0, 1\}^4$ at positions $(0, 1, 2, 3)$ we have that the distance of such a distribution from the uniform distribution is at least $2 \times 2^{-4} = 2^{-3}$.

Hence, assuring that $\delta < 2^{-3}$ we obtain that for each 4 positions there is a nonzero probability of every 4-bit sequence appearing. Hence, for the sequence of random variables Z it holds that every 4-tuple of positions every string out of $\{0, 1, 2, 3\}^4$ appears with non-zero probability.

In our case we need two independent sets of $N = 2^n$ 4-wise $1/8$ -dependent random variables, resulting in a sample space of $O(n^c)$, bearing the desired polynomial construction.

Robustness

Let us assume we would tolerate a failure at most $\frac{(1-f(\epsilon))}{2}l$ devices during the run of the whole protocol. Let us first calculate the number of rounds of the protocol l needed to obtain the original ϵ and δ characteristics of the non-robust device.

Efficiency

Assuming the adversary is cheating (wants to achieve bias greater than ϵ), in each round of the protocol there will be at least one device failure with probability $1-f(\epsilon)$. The probability δ that the adversary stays undetected while all devices produce bias at least ϵ is bounded by the distribution function of the binomial distribution

$$\delta \leq F\left(\frac{(1-f(\epsilon))}{2}l; l; 1-f(\epsilon)\right).$$

This probability can be upper bounded by Chernoff's inequality by

$$F\left(\frac{(1-f(\epsilon))}{2}l; l; 1-f(\epsilon)\right) \leq e^{-\frac{(1-f(\epsilon))}{8}l}. \quad (5)$$

We can derive the necessary number of rounds of the protocol l to be

$$l > 8 \frac{\ln \delta}{f(\epsilon) - 1}.$$

Comparing to the number of rounds needed for the non-robust protocol $\frac{\log \delta}{\log f(\epsilon)}$ we can obtain the scaling factor s to be

$$s = 8 \frac{\ln f(\epsilon)}{f(\epsilon) - 1}.$$

For $f(\epsilon) \rightarrow 1$ (what is the case for small ϵ) the scaling factor approaches a constant of 8.

Imperfectness

We also want to assure there exist a non-zero failing probability of each individual device μ such that the protocol execution will not be (falsely) declared to be attacked by the adversary with high probability. Let us consider an honest provider (not trying to cheat) and set $\mu = \frac{1-f(\epsilon)}{4m}$. We will calculate the probability that more than $\frac{(1-f(\epsilon))}{2}l$ devices will fail during the process.

Since the producer of the devices is assumed to be honest (otherwise the protocol failure is justified), we may assume that failures of devices are independent of each other. Therefore the failures can be modeled by i.i.d. Bernoulli random variables ($Z_i = 1$ if the i -th device fails the test) Z_1, \dots, Z_{ml} , with $P(Z_i = 1) = \mu = \frac{1-f(\epsilon)}{4m}$. The number of failures $Z = \sum_{i=1}^{ml} Z_i$ is binomially distributed. For the protocol not to abort we need less than $\frac{1-f(\epsilon)}{2}l$ failures, hence we need to upper bound the probability

$$P\left(\sum_{i=1}^{ml} Z_i > \frac{1-f(\epsilon)}{2}l\right) = F\left(ml - l \frac{1-f(\epsilon)}{2}, ml, 1-\mu\right).$$

We can use the Hoeffding inequality:

$$P\left(\sum_{i=1}^{ml} Z_i > \frac{1-f(\epsilon)}{2}l\right) \leq e^{-\frac{(1-f(\epsilon))^2}{8m}l},$$

i.e. the probability of false protocol abort drops exponentially with the number of rounds l .

Using H_{full} for Non-Block Sources

We used the following claim in the main text: If we hash the outcome of a (n, Rn) -flat distribution by each of the hash functions from the full set of functions $H_{full} = \{h_i : \{0, 1\}^n \mapsto \{0, 1, 2, 3\}\}$, at least $\frac{Rn}{2}$ functions have uniform and independent outcomes.

First let us suppose Rn is natural and even. Then there are $4^{Rn/2}$ strings appearing with probability $\frac{1}{4^{Rn/2}}$. Let us label them $\{s_i\}_{i=0}^{(4^{Rn/2}-1)}$. We will now explicitly construct hash functions $\{h_j\}_{j=0}^{Rn/2}$ with desired properties.

Let M be $\frac{Rn}{2}$ times $4^{Rn/2}$ matrix with i^{th} column being a representation of i in base 4. Let us assign $h_j(s_i) = M_{ji}$ (example with $Rn = 4$ is depicted in Fig. (3)). Although this is only a partial definition of $\{h_j\}_{j=0}^{Rn/2}$, it is sufficient for our purposes, because other strings appear with probability 0. It should now be straightforward to see that each vector of outcomes $(h_0, \dots, h_{Rn/2})$ appears with equal probability and therefore marginal distributions of outputs of a single function h is uniform and

independent on the others.

	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}
h_0	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
h_1	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3

FIG. 3. Matrix M for $Rn = 4$.

By Caratheodory theorem all other values of Rn can be written as convex combinations of (n, m) flat sources with $m = 2\lfloor Rn/2 \rfloor$, which gives us that the probability to cheat with such (n, Rn) source is at most the same as with (n, m) flat source – i. e. equal to $\lfloor \frac{Rn}{2} \rfloor$ boxes obtaining uniform independent inputs.